31

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/731,039	12/07/2000	Scott A. Moskowitz	031838.0008	1226

45702 7590 06/29/2006

SCOTT A. MOSKOWITZ
16711 COLLINS AVENUE #2505
SUNNY ISLES BEACH, FL 33160

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 06/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/731,039	Applicant(s) MOSKOWITZ ET AL.	
	Examiner Brandon S. Hoffman	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2006*.
2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-68* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-68* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a)☐ All b)☐ Some * c)☐ None of:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-68 are pending in this office action.

2. Applicant's arguments, filed April 10, 2006, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-30, 49-59, and 66-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. (Bender, W., Gruhl, D., Morimoto, N., LU, A.: *Techniques for Data Hiding.* In IBM Systems Journal, vol. 35, no. 3-4. (1996) 313-336) in view of Nagashima et al. (U.S. Patent No. 6,275,988).

Regarding claims 1 and 66, Bender et al. teaches a method/system for securing a data object, comprising:

- Providing an openly accessible data object comprising digital data and file format information (page 313, left column last paragraph, referring to a "host signal");

- Embedding independent data into the openly accessible data object (page 314, left column, items 1 through 6); and
- Where at least a portion of the independent data can be decoded from the scrambled openly accessible data object (page 314, left column, item 6).

Bender et al. does not teach scrambling the openly accessible data object to **perceptibly** degrade the openly accessible data object to a predetermined signal quality level.

Nagashima et al. teaches scrambling the openly accessible data object to **perceptibly** degrade the openly accessible data object to a predetermined signal quality level (col. 7, lines 16-20).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine scrambling the openly accessible data object to degrade the object to a predetermined signal quality level, as taught by Nagashima et al., with the method/system of Bender et al. It would have been obvious for such modifications because degrading the quality level of the signal allows for adjustment for differing image processing apparatuses of end users (see col. 7, lines 6-11 of Nagashima et al.).

Regarding claims 2 and 5, Bender et al. as modified by Nagashima et al. teaches the step of performing the steps of embedding and scrambling until a predetermined condition is met (see col. 7, lines 59-63 of Nagashima et al.).

Regarding claims 3 and 6, Bender et al. as modified by Nagashima et al. teaches the predetermined condition comprises reaching a desired signal quality level of the openly accessible data object (see col. 7, line 64 through col. 8, line 13 of Nagashima et al.).

Regarding claims 4 and 67, Bender et al. as modified by Nagashima et al. teaches the steps of:

- Descrambling the data object to upgrade the openly accessible data object to a predetermined signal quality level (see col. 7, lines 21-38 of Nagashima et al.); and
- Decoding the embedded independent data (see page 314, left column, item 6 of Bender et al.).

Regarding claims 7, 8, 19, and 20, Bender et al. as modified by Nagashima et al. teaches the predetermined signal quality level is selected from **formats of** the group consisting of telephone quality, radio quality, MP3 quality, CD quality, NTSC quality, QuickTime quality, Macrovision quality, satellite quality, high definition quality, and DVD quality (see col. 3, line 66 through col. 4, line 15 of Nagashima et al.).

Regarding claim 9, Bender et al. as modified by Nagashima et al. teaches the independent data comprises authenticatable data (see page 316, right column, LOW BIT RATE DATA HIDING of Bender et al.).

Regarding claims 10 and 23, Bender et al. as modified by Nagashima et al. teaches wherein the authenticatable data comprises a robust open watermark (see page 316, right column, LOW BIT RATE DATA HIDING of Bender et al.).

Regarding claim 11, Bender et al. as modified by Nagashima et al. teaches wherein the step of decoding the embedded independent data comprises using a public key to decode the independent data (see page 317, right column, step 1 of Bender et al).

Regarding claim 12, Bender et al. as modified by Nagashima et al. teaches wherein the openly accessible data object comprises at least one of digital music, video, and at least one image (see page 313, left column, last paragraph of Bender et al.).

Regarding claim 13, Bender et al. as modified by Nagashima et al. teaches the step of scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the openly accessible data object (see page 314, left column, items 1 through 6 of Bender et al. and col. 7, lines 16-20 of Nagashima et al., the order is not specified).

Regarding claims 14 and 68, Bender et al. teaches a method/system for distributing a data signal, comprising:

- Providing a data signal comprising digital data and file format information (page 313, left column last paragraph, referring to a "host signal");
- Where at least a portion of embedded data can be decoded from the scrambled digital signal (page 314, left column, item 6).

Bender et al. does not teach scrambling the data with a first and second scrambling technique.

Nagashima et al. teaches selecting a first scrambling technique to apply to the data signal; scrambling the data signal using the first scrambling technique, resulting in a first-level **perceptibly** degraded data signal; and creating a first descrambling key for the first-level **perceptibly** degraded data signal based on the first scrambling technique (col. 6, line 66 through col. 7, line 5) and selecting a second scrambling technique to apply to the first-level degraded data signal; scrambling the first-level degraded data signal using a second scrambling technique, resulting in a second-level **perceptibly** degraded data signal; and creating a second descrambling key for the second-level **perceptibly** degraded data signal based on the second scrambling technique (col. 6, line 66 through col. 7, line 5).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine first and second scrambling techniques, where the second scrambling technique further scrambles the data of the first scrambling technique, as taught by Nagashima et al., with the method/system of Bender et al. It would have been obvious for such modifications because degrading the quality level of the signal allows for adjustment for differing image processing apparatuses of end users (see col. 7, lines 6-11 of Nagashima et al.).

Regarding claim 15, Bender et al. as modified by Nagashima et al. teaches associating a first payment level with the data signal, a second payment level with a first-level **perceptibly** degraded data signal and a third payment level with a second-level **perceptibly** degraded signal (see fig. 3 of Nagashima et al.).

Regarding claim 16, Bender et al. as modified by Nagashima et al. teaches selecting a payment level; and applying at least one of the descrambling keys to the second-level **perceptibly** degraded data signal, resulting in the associated data signal (see col. 7, lines 59-63 of Nagashima et al.).

Regarding claim 17, Bender et al. as modified by Nagashima et al. teaches at least one of the first scrambling technique and the second scrambling technique comprises manipulation of the file format information (see col. 7, lines 16-21 of Nagashima et al.).

Regarding claim 18, Bender et al. as modified by Nagashima et al. teaches at least one of the first scrambling technique and the second scrambling technique comprises a cryptographic cipher (see col. 20, lines 14-27 of Nagashima et al.).

Regarding claim 21, Bender et al. teaches a method for distributing a data object, comprising:

- Providing a data object comprising digital data and file format information (page 313, left column last paragraph, referring to a "host signal");
- Encoding independent authentication data into the data object (page 314, left column, steps 1 through 6);
- Where at least a portion of the independent authentication data can be decoded from the **perceptibly** manipulated data object (page 314, left column, item 6); and
- Distributing the **perceptibly** manipulated data object where access to the **perceptibly** manipulated data object is not conditional (page 322, second column, DIGITAL WATERMARK paragraph).

Bender et al. does not teach **perceptibly** manipulating the file format information based on at least one signal characteristic of the data object

Nagashima et al. teaches **perceptibly** manipulating the file format information based on at least one signal characteristic of the data object (col. 7, lines 16-20).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine manipulating the file format information based on signal characteristics of the data object, as taught by Nagashima et al., with the method of Bender et al. It would have been obvious for such modifications because creating different levels (or resolutions) of quality allows for adjustment for differing image processing apparatuses of end users (see col. 7, lines 6-11 of Nagashima et al.).

Regarding claim 22, Bender et al. as modified by Nagashima et al. teaches the independent authentication data is steganographically encoded into the data object (see page 315, left column, PRIOR WORK of Bender et al.).

Regarding claim 24, Bender et al. as modified by Nagashima et al. teaches at least one signal characteristic of the data object comprises file format information (see col. 7, lines 16-21 of Nagashima et al.).

Regarding claims 25 and 26, Bender et al. as modified by Nagashima et al. teaches the step of generating at least one cryptographic key based on a result of the manipulation of the file format information comprises selecting at least one of a plurality of signal characteristics of the data format (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.); and ciphering the results of the order of steps of signal characteristic selection (see col. 7, lines 12-15 of Nagashima et al.).

Regarding claims 27 and 28, Bender et al. as modified by Nagashima et al. teaches the steps of encoding independent authentication data into the data object and manipulating the file format information based on at least one signal characteristic of the data object comprise multiple step encoding and manipulation (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.), and an order of the multiple steps is ciphered to generate a predetermined key (see col. 7, lines 12-15 of Nagashima et al.).

Regarding claim 29, Bender et al. as modified by Nagashima et al. teaches generating at least one cryptographic key having a logical relationship with the manipulation of the file format information and the steganographic encoding method (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.).

Regarding claim 30, Bender et al. as modified by Nagashima et al. teaches generating an authorization key that is dependent on a public key and a private key, wherein the authorization key is further dependent on at least one of a time, a channel, and an object (see col. 20, line 55 through col. 21, line 5 of Nagashima et al.).

Regarding claim 49, Bender et al. teaches a method for data signal distribution, comprising:

- Applying a steganographic technique for embedding independent data into the data signal (page 314, left column, steps 1 through 6);

- Where at least a portion of the embedded independent data can be decoded from the scrambled data signal (page 314, left column, item 6).

Bender et al. does not teach applying a scrambling technique selected from the group consisting of file format manipulation and partial encryption and generating a predetermined key based on the embedding and scrambling steps.

Nagashima et al. teaches applying a scrambling technique selected from the group consisting of file format manipulation and partial encryption (col. 7, lines 16-20) and generating a predetermined key based on the embedding and scrambling steps (col. 7, lines 16-20).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine scrambling the data signal and generating a key based on the embedding and scrambling, as taught by Nagashima et al., with the method of Bender et al. It would have been obvious for such modifications because degrading the quality level of the signal allows for adjustment for differing image processing apparatuses of end users (see col. 7, lines 6-11 of Nagashima et al.).

Regarding claim 50, Bender et al. as modified by Nagashima et al. teaches the file format manipulation scrambling technique has a relationship with at least one signal

characteristic of the data signal (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.).

Regarding claim 51, Bender et al. as modified by Nagashima et al. teaches the partial encryption scrambling technique is unrelated to any characteristic of the data signal (see col. 20, lines 55-60 of Nagashima et al.).

Regarding claim 52, Bender et al. as modified by Nagashima et al. teaches the partial encryption scrambling technique degrades a signal quality of the data signal (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.).

Regarding claim 53, Bender et al. as modified by Nagashima et al. teaches the predetermined key enables descrambling of the signal (see col. 20, line 55 through col. 21, line 5 of Nagashima et al.).

Regarding claim 54, Bender et al. as modified by Nagashima et al. teaches the predetermined key is based on unique identifying information for a receiver (see col. 21, lines 1-5 of Nagashima et al.).

Regarding claims 55 and 56, Bender et al. as modified by Nagashima et al. teaches the predetermined key is based on a signal quality threshold that is adjustable in at least one of a time, a frequency, a bit depth, and a measure of payment that may

be adjusted for at least one of a time, a frequency, and a bit depth (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.).

Regarding claim 57, Bender et al. as modified by Nagashima et al. teaches the predetermined key is pre-generated based on at least one expected characteristic of the data signal (see col. 7, lines 16-20 of Nagashima et al.).

Regarding claim 58, Bender et al. as modified by Nagashima et al. teaches the predetermined key is divisible into a plurality of discrete partial keys, each discrete partial key representing less than an entire payment for the data signal (see fig. 3, CHARGE section of Nagashima et al.).

Regarding claim 59, Bender et al. as modified by Nagashima et al. teaches the predetermined key can be broken into a plurality of discrete partial keys, each discrete partial key representing less than an entire descrambled state for the data signal (see fig. 3 of Nagashima et al.).

Claims 60-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. (Bender, W., Gruhl, D., Morimoto, N., LU, A.: *Techniques for Data Hiding*. In IBM Systems Journal, vol. 35, no. 3-4. (1996) 313-336) in view of Nagashima et al. (USPN '988), and further in view of Paterson et al. (U.S. Patent No. 6,051,029).

Regarding claim 60, Bender et al. teaches a method for bandwidth allocation, comprising:

- Presenting a plurality of openly accessible data objects to a user, each data object having a security application (page 313, left column last paragraph, referring to a "host signal"),
- Where the security application comprises embedding, scrambling, or both embedding and scrambling (page 314, left column, steps 1 through 6).

Bender et al. does not teach linking at least a first data object to at least one second data object, wherein a characteristic of the first data object causes a change in the second data object.

Nagashima et al. and Paterson et al. teaches linking at least a first data object to at least one second data object (see col. 6, lines 8-39 of Paterson et al.), wherein a characteristic of the first data object causes a change in the second data object (see fig. 18 of Nagashima et al.).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine linking a first object to a second object, where a change in one object causes a change in the other object, as taught by Nagashima et al./Paterson et al., with the method of Bender et al. It would have been obvious for such modifications because the scalable encoding of Nagashima et al. creates different

levels (or resolutions) of quality that when linked, can be combined to create higher resolution images.

Regarding claim 61, Bender et al. as modified by Nagashima et al./Paterson et al. teaches wherein the first data object comprises advertising (see col. 11, lines 45-52 of Paterson et al.).

Regarding claim 62, Bender et al. as modified by Nagashima et al./Paterson et al. teaches an increased quantity of the first data object causes a signal quality level of the second data object to increase (see fig. 18 of Nagashima et al., more layers give a higher signal quality level).

Regarding claim 63, Bender et al. as modified by Nagashima et al./Paterson et al. teaches a signal quality level of the second data object is increased with a predetermined key (see fig. 18 of Nagashima et al., more layers give a higher signal quality level).

Regarding claim 64, Bender et al. as modified by Nagashima et al./Paterson et al. teaches wherein the predetermined key comprises at least one session key (see fig. 8, 10, and 12 of Nagashima et al.).

Regarding claim 65, Bender et al. as modified by Nagashima et al./Paterson et al. teaches at least one session key adjusts a payment for the second data object (see fig. 3 and 8/10/12 of Nagashima et al.).

Claims 31-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagashima et al. (U.S. Patent No. 6,275,988) in view of Bender et al. (Bender, W., Gruhl, D., Morimoto, N., LU, A.: *Techniques for Data Hiding*. In IBM Systems Journal, vol. 35, no. 3-4. (1996) 313-336).

Regarding claim 31, Nagashima et al. teaches a method for distributing data signals, comprising:

- **Perceptibly** scrambling the data object (col. 7, lines 16-20),
- Distributing the **perceptibly** scrambled data object (fig. 8, 10, 12);
- Distributing at least one predetermined key that enables access to the data object, the embedded independent data, or both the data object and the embedded independent data (col. 6, line 66 through col. 7, line 5); and
- Descrambling the **perceptibly** scrambled data object with the predetermined key (col. 7, lines 21-38).

Nagashima et al. does not teach embedding independent data into a data object, decoding at least a portion of the independent data from the **perceptibly** scrambled

data object with the predetermined key, where at least a portion of the independent data can be decoded from the **perceptibly** scrambled data object.

Bender et al. teaches embedding independent data into a data object (page 314, left column, steps 1 through 6), decoding at least a portion of the independent data from the **perceptibly** scrambled data object with the predetermined key (page 314, left column, item 6), where at least a portion of the independent data can be decoded from the **perceptibly** scrambled data object (page 314, left column, item 6).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine embedding independent data into a data object and decoding at least a portion of the independent data, where at least a portion can be decoded from the scrambled data object, as taught by Bender et al., with the method of Nagashima et al. It would have been obvious for such modifications because embedding and decoding independent data allows copyright detection without preventing distribution of the object (see page 313, left column last paragraph of Bender et al.).

Regarding claim 32, Nagashima et al. as modified by Bender et al. teaches the independent data comprises payment information (see fig. 3, CHARGE of Bender et al.).

Regarding claim 33, Nagashima et al. as modified by Bender et al. teaches wherein the independent data comprises authentication information (see page 316, right column, LOW BIT RATE DATA HIDING of Bender et al.).

Regarding claim 34, Nagashima et al. as modified by Bender et al. teaches the independent data comprises a one-way hash (see page 335, left column, first paragraph of Bender et al.).

Regarding claim 35, Nagashima et al. as modified by Bender et al. teaches the independent data comprises a digital signature (see col. 21, lines 1-5 of Nagashima et al.).

Regarding claim 36, Nagashima et al. as modified by Bender et al. teaches the independent data comprises a time stamp (see col. 21, lines 1-5 of Nagashima et al., digital signatures and time stamps are used for verification).

Regarding claims 37 and 38, Nagashima et al. as modified by Bender et al. teaches the steps of embedding independent data into a data object and scrambling the data object each has a logical relationship with the generation of the predetermined key and a communications channel for which the data signal is being prepared (see col. 6, line 66 through col. 7, line 5 of Nagashima et al.).

Regarding claim 39, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises: initiating the transmission of a recipient public key from an intended recipient of the data object to a sender of the data object; and initiating the transmission of a sender session key from the sender to the recipient to initiate descrambling of the embedded independent data (see fig. 8, 10, and 12 of Nagashima et al.).

Regarding claim 40, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises: initiating a session key-based exchange between a sender and receiver; wherein the session key is dependent on at least one of a channel, a time, and a data object (see fig. 8, 10, and 12 of Nagashima et al.).

Regarding claim 41, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises initiating a session key-based exchange between a sender and a receiver that is a timing based timing mechanism (see fig. 8, 10, and 12 of Nagashima et al., a web-based environment would require a session key-based exchange).

Regarding claim 42, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises initiating a pooling of similar session keys (see col. 20, lines 15-32 of Nagashima et al.).

Regarding claim 43, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises logically associating a signal quality with a predetermined estimation of a bandwidth requirement for the session (see col. 7, lines 6-11 of Nagashima et al.).

Regarding claim 44, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises logically associating a signal quality with a bandwidth allocation model (see col. 7, lines 6-11 of Nagashima et al.).

Regarding claim 45, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises logically associating a signal quality with a signal quality parameter (see fig. 3 of Nagashima et al.).

Regarding claim 46, Nagashima et al. as modified by Bender et al. teaches the step of descrambling the scrambled data object comprises updating a signal quality of the data object based on an approval of the session keys by the originating data signal server (see col. 7, lines 21-38 of Nagashima et al.).

Regarding claim 47, Nagashima et al. as modified by Bender et al. teaches wherein the step of scrambling the data object comprises manipulating file format information of the data object (see col. 7, lines 16-21 of Nagashima et al.).

Regarding claim 48, Nagashima et al. as modified by Bender et al. teaches wherein the step of scrambling the data object comprises scrambling the data object with a cryptographic cipher (see col. 20, lines 14-27 of Nagashima et al.).

Response to Arguments

5. Applicant argues, both here and in previous interviews, that scrambling the openly accessible data object to **perceptibly** degrade the openly accessible data object to a predetermined signal quality level meant that whatever file format that the data object was in, scrambling to degrade the data object would keep the data object in the same file format, but add distortions. For example, an audio file, according to the applicant, in MP3 file format, is scrambled to degrade. Applicant explained to examiner that the scrambling would leave the audio file in MP3 file format, but would add noises, like popping, and other distortions. If the data object were a video, such as DVD format, scrambling would leave the file as DVD format, but add blurriness or other distortions.

During examination of the claims, the examiner was under the impression that scrambling to degrade meant that an audio file in MP3 file format would be degraded down to radio quality and be further degraded to telephone quality. Upgrading the audio file would return the telephone quality file to radio quality, and then eventually to MP3 quality. Examiner's art rejection reflected this misinterpreted fact.

Regarding applicants argument, examiner disagrees. Examiner would like to point out page 19, lines 26-31 of applicant's disclosure. The paragraph explains that

scrambling to degrade takes a CD quality audio file and reduces it to MP3, from MP3 to FM, from FM to AM, and from AM to telephone. Similar steps are taken for a video file. This clearly shows that the scrambling to degrade step involves changing the file format from one format (MP3) to another format (FM) as examiner had previously thought. The applied references, namely Nagashima et al., teach a lower grade quality file that is for little or no charge, a middle grade quality file for medium charge, and a high grade quality file for a high charge.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100